INL/MIS-24-77369-Revision-0



# Interdisciplinary Approaches to Cybervulnerability Impact Assessment for Energy Critical Infrastructure

May 2024

Andrea NMN Gallardo

Changing the World's Energy Future

Idaho National Laboratory

*INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC*

INL/MIS-24-77369-Revision-0

# Interdisciplinary Approaches to Cybervulnerability Impact Assessment for Energy Critical Infrastructure

**Andrea NMN Gallardo**

**May 2024**

**Idaho National Laboratory**
**Idaho Falls, Idaho 83415**

**http://www.inl.gov**

**Prepared for the**
**U.S. Department of Energy**
**Under DOE Idaho Operations Office**
**Contract DE-AC07-05ID14517, DE-AC07-05ID14517**

# Interdisciplinary Approaches to Cybervulnerability Impact Assessment for Energy Critical Infrastructure

**Andrea Gallardo**, Robert Erbes, Katya LeBlanc,

Lujo Bauer, and Lorrie Cranor

2024 ACM SIGCHI

Idaho National Laboratory INL

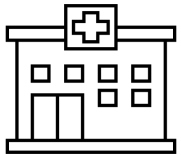
CyLab Carnegie Mellon University Security and Privacy Institute

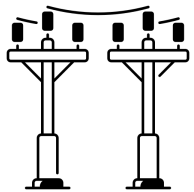
# Protecting Energy Infrastructure

Disruptions to the energy grid can have severe consequences.

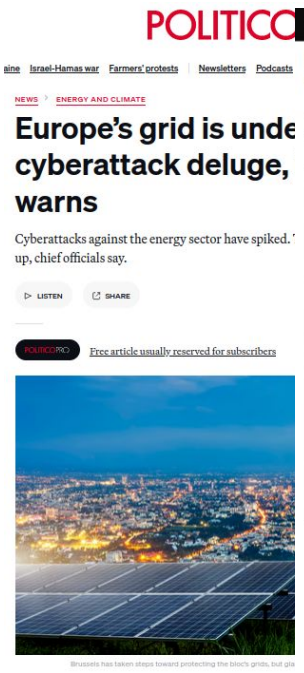
The loss of power can cause a ripple effect:

- Hospitals
- Financial services
- Agriculture
- Energy production
- Energy distribution





# Attacks on the Energy Grid

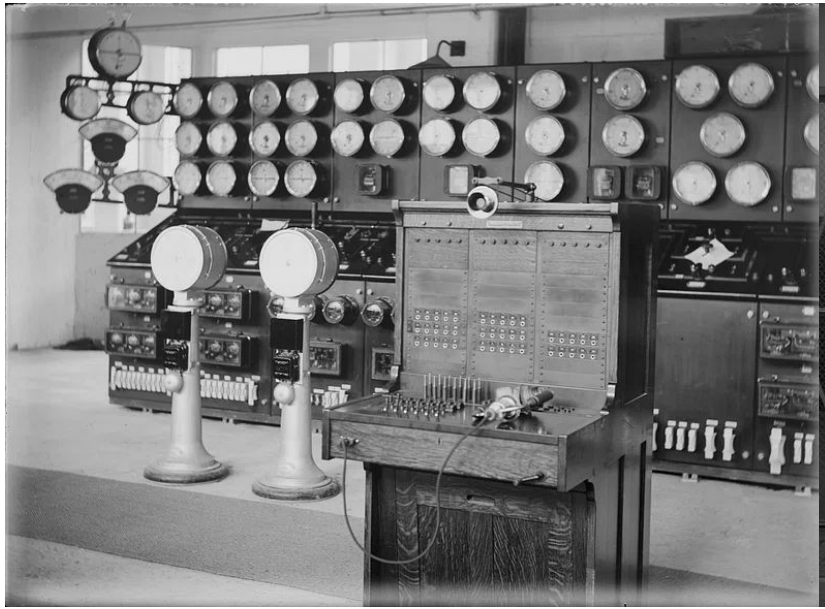


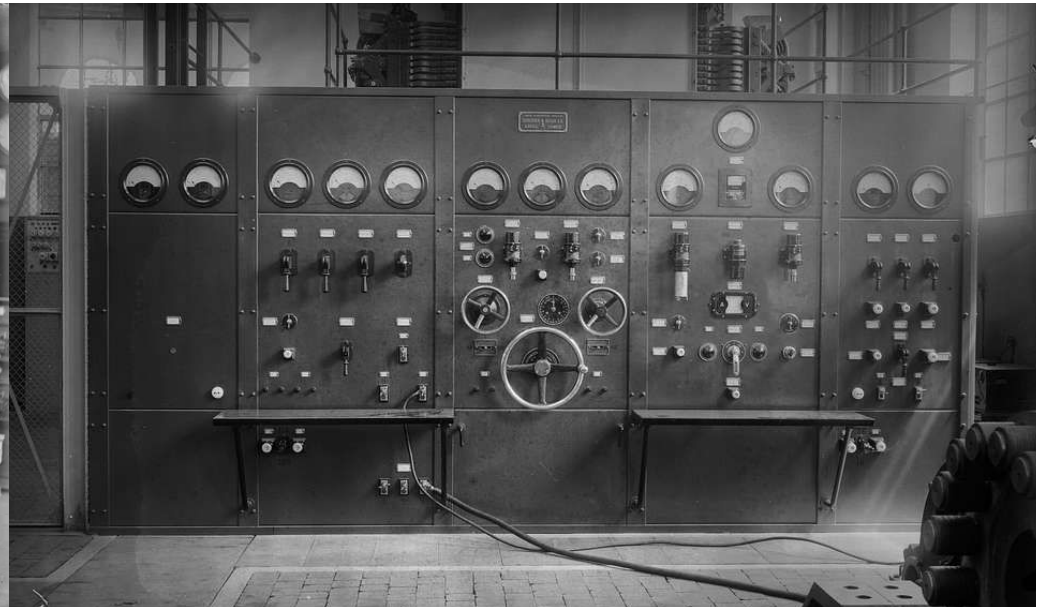



Cars lined up for gasoline in Charlotte, N.C., on Tuesday. Logan Cyrus/Agence France-Presse — Getty Images

Sources:https://www.politico.eu/article/energy-power-europe-grid-is-under-a-cyberattack-deluge-industry-warns/, https://www.nytimes.com/2021/05/13/climate/pipeline-ransomware-hack-energy-grid.html
https://www.cnn.com/2022/12/27/politics/hackers-data-utilities-ransomware-sargent-lundy/index.html,
https://www.zdnet.com/article/critical-infrastructure-is-under-attack-from-hackers-securing-it-needs-to-be-a-priority-right-now

# Traditional Energy Grid Security





Images: Leslie Adkin - Museum of New Zealand (Source), Swiss Federal Railways via Picryl.com

# Networked Energy Infrastructure

Smart meters


Laptops

Sensors

Images: EVB Energy Ltd https://de.wikipedia.org/wiki/Image:Zaehler.jpg
Defense Visual Information Distribution Service https://images.app.goo.gl/Kgey5KQ7QJonDqMn8
Stephan Brosnan, CSIRO http://www.scienceimage.csiro.au/image/3876

# Energy Infrastructure Increasingly Vulnerable

Energy OT increasingly **vulnerability to cyber attacks**:

- **Exploitation** of computer vulnerabilities
- Shortage of **computer security professionals**

# Challenges Defending Energy Infrastructure

- **Legacy systems**
  - Vulnerable to known exploits
- Need to **operate continuously**
  - Delay patching and updates
- **Small utilities** may lack resilient defenses and recovery plans
  - Limited resources

# Understanding Energy Production Processes

Generation

Transmission

Distribution

Images: rawpixel.com / Carol M Highsmith https://images.app.goo.gl/88zwd3BKBEufPfFz5, Oran Viriyincy https://images.app.goo.gl/dxbns8jEJMQ2dFkk7, Pix4free https://images.app.goo.gl/WsPrUjSd6AmSFyeaA

# Cross-Domain Knowledge & Collaboration

Different security approaches in IT and OT contexts:

- Differences in training, knowledge, and culture
- Regulations for IT security versus OT safety
- Conflicts between IT policies and OT continual operations

Need cross-domain knowledge:

- Help energy OT professionals address cyber risk
- Help computer security professionals develop relevant security measures

# Subject Matter Experts (SMEs)

**Energy OT SMEs**

Operational technology experts with experience in energy systems engineering and operations

**Cyber SMEs**

Computer security experts who research industrial control system security

# Research Questions

RQ1: What information do cyber SMEs and energy SMEs need when assessing the potential impact of computer vulnerabilities? Are there notable differences between the groups?

RQ2: What are their perceptions of differences between the two groups' approaches to impact assessment and understanding of vulnerabilities?

RQ3: What suggestions do they have for collaboration between the two groups or building cross-domain understanding?

# Methodology: Interviews

Semi-structured **interviews** with 18 subject matter experts (SMEs):

- Virtual
- 60-90 minutes
- 18 employees of an energy-sector organization
  - All had interdisciplinary experience

# Methodology: Qualitative Data Analysis

**Qualitative coding** of interview transcripts:

- *A priori* codes related to computer security and vulnerabilities
- Emergent codes:
    - **Stereotype**: tendency for a SME group to do certain things or see things a certain way
    - **Occupational Motivation**: habits, mindset or approaches based on training or job; what they are expected to do
    - **Suggestion**: recommendation regarding interdisciplinary work or collaboration

# Methodology: Analyzing Expert Approaches

Interviews explored:

- Information necessary for assessing vulnerability impact
  - Unprompted self-reported approach
  - Prompted about factors: subsector, vendor
- Perceptions of each expert group (energy OT and cyber)
  - Approaches to impact assessment
  - Understanding of vulnerabilities

# Results: Summary

**Similarities**:

- General considerations for vulnerability impact assessment
- Displayed cross-domain knowledge

**Differences**:

- Domain-specific perspectives

**Energy OT**: System-wide

**Cyber**: Adversarial

**Stereotypes**: Perceptions of domain-specific mindset and skills

**Suggestions**: More interdisciplinary collaboration & education

# Cross-domain Knowledge

*Energy OT SME recognizes exploitability of OT equipment:*

"From the perspective of the maker, the people who install it, [and] the protection and controls people," **a protective relay** is a device that quickly and reliably "**reads electrical voltage and current**," then "does some math on them" to determine whether or not "to **send a trip signal to a breaker.** … From the adversary, cyber security perspective, **this thing is a computer.** It's got a full-blown **operating system**. … If I have the right passwords or I can figure out how to **bypass the different protections** on it, I can make this thing do anything that a computer could do." (E7)

# Cross-domain Knowledge

*Cyber SME recognizes need to debug OT equipment:*

"If there's an **exposed port** that you can connect to that **gives you debug access or a shell,** that would largely be an issue with a consumer device, because that means your consumer could do whatever the heck they want to with your device. But in the case of a **high reliability system in generation**, it might be significantly more important to have that as a means of **debugging** any issues that do occur with the device." (C17)

# Cyber SME Focus

Adversarial focus:

- Gaining access
- Identifying connections
- Modifying device capabilities
- Considering exploit details

# Cyber SME Focus

**Energy OT**: *Is it exploitable?*

**Cyber**: *How **easy** is it to exploit?*

- Difficulty
- How reachable the system is
- Attacker's skill level

Adversarial focus:

- Gaining access
- Identifying connections
- Modifying device capabilities
- **Considering exploit details**

# Cyber SME Focus

"I would try to **trace a path** to this piece of equipment to try to understand how easy it is to get there. Some equipment is designed to be on **a network that is more likely to have malicious traffic**. Other equipment is not designed for that, and it's expected that it's going to be behind several **firewalls**. (C12)"

Adversarial focus:

- Gaining access
- **Identifying connections**
- Modifying device capabilities
- Considering exploit details

# Energy OT SME Focus

Holistic system-level focus:

- **Connections to larger system**
- Disruption in operations
- Risk mitigation

*Distribution systems "becoming more integrated":*

*"Historically, a distribution system was one radial feed. Now it's starting to talk to all the meters out in these residential areas." (E8)*

# Energy OT SME Focus

Holistic system-level focus:

- **Connections to larger system**
- Disruption in operations
- Risk mitigation

*Is the location a "high priority site" that needs to "maintain critical loads" i.e., would it be among the last users to lose service and among the first users returned to service after an interruption? (E15)*

# Complementary Approaches

Cross-domain interaction

Exposure to other methods & mindsets

Building overlap in understanding risk

# Recommendations

Suggestions made by participants:

- Interdisciplinary communication and knowledge sharing:
  - Integrate siloed teams in energy OT environments
  - Hold conversations that build mutual understanding
  - Conducting red-team simulated attack exercises

# Future Work

Effective and scalable cross-domain knowledge transfer

- **Interventions**: training, educational materials or interdisciplinary interactions with a domain expert
- **Other topics**: acceptable risk, acceptable mitigations, patching, etc.

Studies with **experts lacking cross-domain experience**

- Might find starker differences in approaches

Large-scale survey to test hypothesis:

- Does **interdisciplinary background** results in similar considerations?

# Interdisciplinary Approaches to Cybervulnerability Impact Assessment for Energy Critical Infrastructure

**Andrea Gallardo**, Robert Erbes, Katya LeBlanc,
Lujo Bauer, and Lorrie Cranor

- Our study characterizes experts' approaches to impact assessment in energy OT contexts and differences in perspectives
- Recommend un-siloing teams, holding conversations, & training
- Future research with non-interdisciplinary experts

Idaho National Laboratory INL

CyLab Carnegie Mellon University Security and Privacy Institute

WEBVTT

1
00:00:06.090 --> 00:00:27.110
Andy: Hello! My name is Andy Gallardo. I'm a Phd. Student at Carnegie Mellon University, and I'll be presenting a talk for our paper Interdisciplinary approaches to cyber vulnerabilities, impact assessment for energy, critical infrastructure. This work was done with my collaborators. Robert Erbes, Katya LeBlanc Lujo Bauer and Lorrie Cranor

2
00:00:29.070 --> 00:00:33.580
Andy: Protection of energy infrastructure is an immensely critical security problem.

3
00:00:33.680 --> 00:00:38.240
Andy: Disrupting energy grid operations can have severe consequences for society.

4
00:00:38.380 --> 00:00:50.680
Andy: The loss of power can cause ripple effects that impact other critical sectors and services, such as hospitals, financial services, agriculture and energy production and distribution

5
00:00:51.800 --> 00:00:55.010
Andy: attacks on the energy grid are becoming increasingly common

6
00:00:55.100 --> 00:00:58.169
Andy: and highlight the growing threat to critical infrastructure.

7
00:00:58.320 --> 00:01:04.280
Andy: Here are just a few of the many news headlines about attacks on the energy grid in the past few years.

8
00:01:06.480 --> 00:01:14.309
Andy: Traditionally, energy systems were independent of information technology or relied on blocking connections to external networks.

9
00:01:14.440 --> 00:01:22.410
Andy: In energy operational contexts, the security of operational equipment was considered in terms of equipment, failure or misuse.

10
00:01:24.030 --> 00:01:36.990

Andy: However, energy, grid infrastructure increasingly relies upon computers and computer networks to operate with operational technology, now including network devices such as smart meters, laptops and wireless sensors.

11
00:01:38.300 --> 00:01:47.019
Andy: With this growing reliance on networks, energy OT infrastructure becomes increasingly vulnerable to cyber attacks through exploitation of computer vulnerabilities.

12
00:01:47.320 --> 00:01:57.960
Andy: Additionally, there is a well documented shortage of computer security security professionals generally. So it is not possible to just hire lots of cybersecurity staff.

13
00:01:58.000 --> 00:02:01.250
Andy: even if that's something that all utilities could afford

14
00:02:02.850 --> 00:02:12.579
Andy: IT security approaches are often inadequate for energy operational contexts which face challenges, such as legacy systems that run on old operating systems

15
00:02:12.760 --> 00:02:20.840
Andy: which make them vulnerable to known exploits as well as the need to operate continuously, which can delay patching and updates.

16
00:02:21.350 --> 00:02:32.120
Andy: Furthermore, smaller energy facilities and utilities may lack resilient defenses and recovery plans due to limited financial staffing and computer security resources

17
00:02:33.870 --> 00:02:37.870
Andy: protecting the power grid is not limited to understanding vulnerabilities.

18
00:02:37.900 --> 00:02:46.139
Andy: It also requires an understanding of how its operational technology contributes to the generation transmission and distribution of energy.

19
00:02:46.180 --> 00:02:49.049
Andy: And if how computer vulnerabilities can impact

20

00:02:49.210 --> 00:02:52.119
Andy: these energy production processes

21
00:02:54.850 --> 00:03:05.600
Andy: while defending the energy grid requires understanding both domains. Prior work has shown that there are major differences in securing information technology and securing operational technology.

22
00:03:05.670 --> 00:03:13.590
Andy: including differences in workers training, knowledge and culture regulations for IT security versus OT safety,

23
00:03:13.810 --> 00:03:18.989
Andy: and conflicts between it policies and ot continual operations.

24
00:03:19.650 --> 00:03:26.239
Andy: So what can utilities and power plants do to secure energy ot as it increasingly involves it.

25
00:03:27.020 --> 00:03:35.699
Andy: One approach is to foster collaboration between energy operators and computer security professionals in order to build cross domain knowledge.

26
00:03:35.830 --> 00:03:45.069
Andy: such cross domain knowledge will help energy ot professionals make better informed decisions about how to address risks posed by computer vulnerabilities,

27
00:03:45.420 --> 00:03:51.839
Andy: and also help computer security experts develop security measures that are suitable for energy environments.

28
00:03:51.880 --> 00:03:55.450
Andy: whether on-site or designing industry-wide standards.

29
00:03:57.120 --> 00:04:02.199
Andy: In our study, we're concerned with 2 types of subject matter experts or SMEs

30
00:04:02.390 --> 00:04:11.629
Andy: we refer to as energy Ot SMEs, who are operational technology experts with experience in energy systems, engineering and operations

31
00:04:11.810 --> 00:04:13.160
Andy: and Cyber SMEs

32
00:04:13.180 --> 00:04:17.639
Andy: computer security experts who research, industrial control system security.

33
00:04:19.850 --> 00:04:27.340
Andy: Our work aims to shed light on these differences with the aim of helping
Foster cross domain knowledge and collaboration.

34
00:04:27.850 --> 00:04:30.259
Andy: Our research questions were one.

35
00:04:30.430 --> 00:04:37.190
Andy: What information do cyber SMEs and energy SMEs need when assessing the
potential impact of computer vulnerabilities?

36
00:04:37.210 --> 00:04:40.079
Andy: Are there notable differences between the 2 groups?

37
00:04:40.750 --> 00:04:41.660
Andy: 2.

38
00:04:41.810 --> 00:04:49.499
Andy: What do these experts consider to be the differences between the 2 groups
approaches to impact assessment and understanding of vulnerabilities?

39
00:04:50.870 --> 00:04:51.780
Andy: 3.

40
00:04:52.170 --> 00:04:58.779
Andy: What insights or suggestions do these experts provide that directly address
collaboration between the 2 groups.

41
00:04:59.080 --> 00:05:01.449
Andy: for building cross-domain understanding.

42

00:05:03.760 --> 00:05:05.760
Andy: We conducted semi-structured

43
00:05:05.780 --> 00:05:09.289
Andy: virtual interviews with 18 subject matter experts

44
00:05:09.320 --> 00:05:11.470
Andy: lasting 60 to 90 min.

45
00:05:11.870 --> 00:05:16.290
Andy: All participants were employees of an energy sector organization.

46
00:05:16.310 --> 00:05:20.829
Andy: and all of them had interdisciplinary experience. Working with the other kind of SME

47
00:05:24.180 --> 00:05:28.410
Andy: to analyze the interview transcripts we conducted qualitative coding.

48
00:05:28.520 --> 00:05:37.920
Andy: developing 2 codebooks, one with a priori codes for impact assessment strategy topics related to computer security and vulnerabilities.

49
00:05:38.690 --> 00:05:42.410
Andy: The other codebook contained themes that emerged from the transcripts

50
00:05:42.430 --> 00:05:44.779
Andy: which we sorted into 3 categories.

51
00:05:44.990 --> 00:05:46.210
Andy: stereotype

52
00:05:46.470 --> 00:05:48.339
Andy: occupational motivation

53
00:05:48.540 --> 00:05:49.930
Andy: and suggestion.

54

00:05:53.210 --> 00:06:01.689
Andy: following the research questions our interviews explored. What information energy OT SMEs and cyber SMEs found necessary to assess impact.

55
00:06:02.030 --> 00:06:07.470
Andy: We asks both unprompted, open-ended questions to capture their self-reported approach.

56
00:06:07.490 --> 00:06:11.070
Andy: and prompted questions about factors that might influence their approach.

57
00:06:11.460 --> 00:06:16.949
Andy: We also asked participants for their perspectives on how each group, their own and the other group,

58
00:06:17.070 --> 00:06:21.319
Andy: approach to impact assessment, and how well each group understood vulnerabilities.

59
00:06:23.560 --> 00:06:30.839
Andy: We expected cyber sneeze, and energy. Ot snees to show a stark imbalance in their approaches to vulnerability impact assessment.

60
00:06:31.010 --> 00:06:37.949
Andy: But we did not find this to be the case when self-reporting their approaches, both groups responded similarly at a general level.

61
00:06:38.150 --> 00:06:45.010
Andy: Both groups also displayed knowledge about both domains, perhaps due to their interdisciplinary work at the same organization.

62
00:06:45.860 --> 00:06:51.820
Andy: Yet we also observed notable differences in the details of their self-reported considerations.

63
00:06:52.220 --> 00:06:55.549
Andy: while cyber SMEs displayed a more adversarial focus

64
00:06:55.690 --> 00:06:59.780
Andy: energy SMEs focused on holistic, system-wide considerations.

65
00:07:01.200 --> 00:07:09.790
Andy: stereotypes that participants conveyed about each group included the idea that cyber SMEs tend to protect systems by cutting off access

66
00:07:10.090 --> 00:07:15.980
Andy: and that energy. OT. Screens take shortcuts and bypass security measures for the sake of convenience.

67
00:07:16.470 --> 00:07:19.720
Andy: You can find more details about these stereotypes in the paper.

68
00:07:20.260 --> 00:07:25.209
Andy: Finally, we collected participants suggestions for interdisciplinary collaboration

69
00:07:25.280 --> 00:07:27.490
Andy: which we will discuss at the end of this talk

70
00:07:29.150 --> 00:07:32.270
Andy: as we dive into some of the participants' responses.

71
00:07:32.410 --> 00:07:41.579
Andy: I want to highlight that not only did our participants show similarities in their impact assessment approaches, they also displayed cross domain awareness in their responses.

72
00:07:41.810 --> 00:07:48.399
Andy: for example, energy, OT SME E7 understood the exploitability of OT. Equipment.

73
00:07:48.650 --> 00:07:49.590
Andy: saying.

74
00:07:49.850 --> 00:07:55.329
Andy: from the perspective of the Maker, people who install it and the protection and controls people.

75
00:07:55.380 --> 00:08:04.549

Andy: a protective relay is a device that quickly and reliably reads electrical voltage and current. Then does some math on them to determine whether or not to send a trip signal to a breaker

76
00:08:05.090 --> 00:08:08.220
Andy: from the adversary cybersecurity perspective.

77
00:08:08.240 --> 00:08:09.780
Andy: This thing is a computer.

78
00:08:09.810 --> 00:08:17.250
Andy: It's got a full blown operating system. If I have the right passwords, or I can figure out how to bypass the different protections on it.

79
00:08:17.260 --> 00:08:20.120
Andy: I can make this thing do anything that a computer could do

80
00:08:22.350 --> 00:08:25.869
Andy: in contrast to the stereotype of wanting to block connections.

81
00:08:25.930 --> 00:08:34.760
Andy: Cyber SME C17 was able to recognize the importance of having debugging access for operators of an energy system, saying.

82
00:08:35.000 --> 00:08:39.799
Andy: if there's an exposed port that you can connect to that gives you debug access or a shell

83
00:08:39.960 --> 00:08:42.669
Andy: that would largely be an issue with a consumer device.

84
00:08:42.730 --> 00:08:46.750
Andy: because that means your consumer could do whatever the heck they want to with your device.

85
00:08:46.930 --> 00:08:50.430
Andy: But in the case of a high reliability system and generation

86
00:08:50.440 --> 00:08:56.579

Andy: it might be significantly more important to have that as a means of debugging any issues that do occur with a device.

87
00:08:59.180 --> 00:09:01.530
Andy: Now, I will highlight some of the differences

88
00:09:01.690 --> 00:09:04.500
Andy: and domain. Specific perspectives of each group

89
00:09:04.820 --> 00:09:10.989
Andy: finding differences within this interdisciplinary group of participants is particularly insightful

90
00:09:11.100 --> 00:09:17.219
Andy: as the differences highlight emphases and mindsets that can persist despite cross domain experience.

91
00:09:20.730 --> 00:09:27.080
Andy: first, cybers SMEs' adversarial focus address, gaining access to networks and resources.

92
00:09:27.220 --> 00:09:29.910
Andy: tracing paths across boundaries.

93
00:09:30.090 --> 00:09:34.360
Andy: modifying devices and their functionality and exploitability.

94
00:09:37.230 --> 00:09:41.720
Andy: for example, of the participants who discussed exploit details.

95
00:09:41.780 --> 00:09:46.430
Andy: All 5 Cyber SMEs asked how easy it would be to exploit the vulnerability.

96
00:09:46.870 --> 00:09:50.930
Andy: while 2 energy OT SMEs asked whether it was actually exploitable.

97
00:09:51.340 --> 00:09:55.699
Andy: Cyber SMEs; responses implied that compromise was possible.

98
00:09:55.710 --> 00:10:03.349
Andy: but that their consideration depended on difficulty. Highlighting factors like how reachable the system is, and the attacker's skill level.

99
00:10:05.540 --> 00:10:10.690
Andy: The more holistic emphases of energy OT SMEs focused on the overall system.

100
00:10:10.810 --> 00:10:13.230
Andy: potential disruptions and operations

101
00:10:13.280 --> 00:10:17.570
Andy: and risk mitigation. For example, energy SME E8

102
00:10:17.680 --> 00:10:22.270
Andy: expressed concerns about distribution systems becoming more integrated.

103
00:10:22.920 --> 00:10:27.380
Andy: saying historically, a distribution system was one radio feed.

104
00:10:27.600 --> 00:10:32.150
Andy: Now it's starting to talk to all the meters out in these residential areas.

105
00:10:34.470 --> 00:10:55.649
Andy: Energy OT SMEs also spoke in more detail about potential disruptions and operations. For example, participant E15 considered whether the location might be a high priority site that needs to maintain critical loads, and thus, whether it would be among the last users to lose service, and among the first users returned to service after an interruption.

106
00:10:57.950 --> 00:11:03.990
Andy: These different groups of experts can potentially complement each other in cross-domain interactions by

107
00:11:04.010 --> 00:11:07.869
Andy: providing exposure to other methods and other ways of thinking

108
00:11:07.900 --> 00:11:12.020
Andy: and building overlap in understanding risks for energy OT systems.

109
00:11:12.680 --> 00:11:23.969
Andy: For example, cross-domain knowledge could help operators interpret computer security standards with more nuance rather than mechanically following checklists or output from automated systems.

110
00:11:24.070 --> 00:11:28.719
Andy: thus building resiliency in the human operators of energy OT systems.

111
00:11:32.300 --> 00:11:39.260
Andy: participants' own interdisciplinary experience informed their recommendations for cross-domain interactions.

112
00:11:39.690 --> 00:11:48.639
Andy: We echo participants' suggestions addressing collaboration between the 2 groups, such as the integration of siloed teams who could learn from each other.

113
00:11:49.050 --> 00:11:52.219
Andy: holding conversations that build mutual understanding

114
00:11:52.390 --> 00:11:55.900
Andy: and conducting red team simulated attack exercises

115
00:12:00.310 --> 00:12:03.090
Andy: given limited resources and labor supply.

116
00:12:03.130 --> 00:12:13.690
Andy: We also encourage the design and development of tools and interventions that could help to effectively and scalably enable cross-domain knowledge transfer in energy Ot contexts.

117
00:12:15.270 --> 00:12:19.659
Andy: Such work could also explore topics such as acceptable risk mitigations.

118
00:12:19.810 --> 00:12:23.220
Andy: risk, mitigations, patching and patching.

119
00:12:23.620 --> 00:12:30.300
Andy: We also encourage future work, interviewing or surveying experts who lack cross domain experience

120
00:12:30.340 --> 00:12:34.199
Andy: to see whether starker differences and approaches in understanding appear

121
00:12:34.890 --> 00:12:44.500
Andy: finally, a larger scale survey might be able to shed light on our hypothesis that the interdisciplinary background of our participants led them to have similar responses.

122
00:12:48.180 --> 00:13:01.009
Andy: In conclusion, our findings, characterize experts' approaches to impact assessments in energy OT contexts and highlight differences in focus, mindset and understanding of energy OT SMEs and cyber SMEs.

123
00:13:01.550 --> 00:13:07.459
Andy: The problem remains that in practice cybers SMEs and energy SMEs often lack cross domain knowledge.

124
00:13:07.560 --> 00:13:11.520
Andy: echoing suggestions made by our interdisciplinary participants.

125
00:13:11.700 --> 00:13:14.590
Andy: We recommend bringing existing teams together,

126
00:13:14.730 --> 00:13:18.679
Andy: fostering cross domain conversations and developing relevant training.

127
00:13:19.080 --> 00:13:25.479
Andy: We are also interested in future work exploring the perspectives of experts without interdisciplinary experience.

128
00:13:25.790 --> 00:13:28.129
Andy: Thank you for listening to my presentation.